

IN THE CLAIMS

Please amend the claims as follows:

Claim 1 (Currently Amended): A computer-readable storage medium, comprising:

a first execution file recorded on said computer-readable storage medium using a copy protection mechanism, said first execution file including

instructions for performing an authentication process with a second execution file,

instructions for obtaining unique key information unique to said first execution file, and

instructions for transmitting said unique key information to said second execution file,

wherein the instructions for performing, instructions for obtaining, and instructions for transmitting in said first execution file are executed by an information processing apparatus including a processor, when said computer-readable storage medium is inserted into said information processing apparatus, and said second execution file generates a content key from said transmitted unique key information, decrypts encrypted content using the content key, and reproduces the decrypted content, and

wherein said encrypted content is recorded on said computer-readable storage medium and said unique key information is configured to encrypt encryption key information which is used for encrypting digital signature information that has previously been attached to said encrypted content, and said instructions for transmitting cause said encrypted content to be transmitted to said second execution file based on said digital signature information.

Claim 2 (Previously Presented): The computer-readable storage medium as claimed in claim 1, wherein said unique key information is used to encrypt encryption key information for encrypting a content.

Claim 3 (Previously Presented): The computer-readable storage medium as claimed in claim 2, wherein at least one of said second execution file and said encrypted content is recorded on said computer-readable storage medium.

Claim 4 (Canceled).

Claim 5 (Currently Amended): An information processing apparatus into which a computer-readable storage medium is inserted, said computer-readable storage medium including a first execution file recorded using a copy protection mechanism, said information processing apparatus comprising:

a processor; and

a second execution file for reproducing an encrypted content,

wherein said second execution file includes instructions for performing an authentication process with said first execution file, instructions for generating encryption key information based on unique key information that is obtained from said first execution file, instructions for decrypting said encrypted content using said encryption key information, and instructions for reproducing the decrypted content, and wherein said second execution file is executed when said computer-readable storage medium is inserted into the information processing apparatus, and

wherein said encrypted content is recorded on said computer-readable storage medium and said unique key information is configured to encrypt encryption key information

which is used for encrypting digital signature information that has previously been attached to said encrypted content, and ~~said~~ instructions for transmitting cause said encrypted content to be transmitted to said second execution file based on said digital signature information.

Claim 6 (Currently Amended): The information processing apparatus as claimed in claim 5, wherein said encrypted content is recorded on one of said computer-readable storage medium, recorded in said information processing apparatus, and recorded in a different information processing apparatus.

Claim 7 (Previously Presented): The information processing apparatus as claimed in claim 5, wherein said encrypted content is recorded on said computer-readable storage medium, said unique key information is used to encrypt encryption key information for encrypting digital signature information attached to said encrypted content, and said second execution file can receive said encrypted content from said first execution file based on said digital signature information.

Claim 8 (Currently Amended): An information processing method implemented by an information processing apparatus into which a computer-readable storage medium is inserted, said computer-readable storage medium having a first execution file recorded therein using a copy protection mechanism, said information processing method comprising:
performing, by a processor in the information processing apparatus, an authentication process with said first execution file;

generating, by the processor in the information processing apparatus, encryption key information based on unique key information that is obtained from said first execution file;

decrypting, by the processor in the information processing apparatus, an encrypted content using said encryption key information;

recording, ~~with~~ by the processor in the information processing apparatus, said decrypted content on said computer-readable storage medium;

reproducing the decrypted content with the information processing apparatus;

using unique key information to encrypt encryption key information for encrypting digital signature information attached to said encrypted content; and

transmitting said encrypted content to said second execution file based on said digital signature information.

Claim 9 (Previously Presented): The computer-readable storage medium as claimed in claim 2, wherein at least one of said second execution file and said encrypted content is recorded in said information processing apparatus.

Claim 10 (Previously Presented): The computer-readable storage medium as claimed in claim 2, wherein at least one of said second execution file and said encrypted content is recorded in a different information processing apparatus.

Claim 11 (Canceled).

Claim 12 (Currently Amended): A computer-readable storage medium, comprising:
a first execution file configured to be executed, by an information processing apparatus including a processor, when the computer-readable storage medium is inserted into the information processing apparatus, ~~the first execution file being copy protected,~~

wherein, in response to executing the first execution file, unique key information is transferred to a second execution file, the second execution file configured to verify digital ~~signature~~ authentication information attached to a content downloaded via a network by using unique key information, decrypt the content, and reproduce the decrypted content.